

BÁO CÁO THỰC HÀNH

Môn học: **Hệ thống tìm kiếm, phát hiện và ngăn ngừa xâm nhập**

Lab 03 – Viết rules trên Snort

GVHD: Đỗ Hoàng Hiển

1. **THÔNG TIN CHUNG:**

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT204.021.ANTT.2

STT	Họ và tên	MSSV	Email
1	Nguyễn Viết Dũng	21520747	21520090@gm.uit.edu.vn
2	Lưu Thị Huỳnh Như	21521242	21521112@gm.uit.edu.vn
3	Lê Đoàn Trà My	21521149	21521149@gm.uit.edu.vn

2. **NỘI DUNG THỰC HIỆN:**¹

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1.1	100%
2	Yêu cầu 1.2	100%
3	Yêu cầu 1.3	100%
4	Yêu cầu 1.4	100%
5	Yêu cầu 1.5	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

¹ Ghi nội dung công việc, yêu cầu trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Yêu cầu 1.1: Giới hạn gói tin đến dịch vụ DNS đến máy Victim: không quá 90 gói/10s

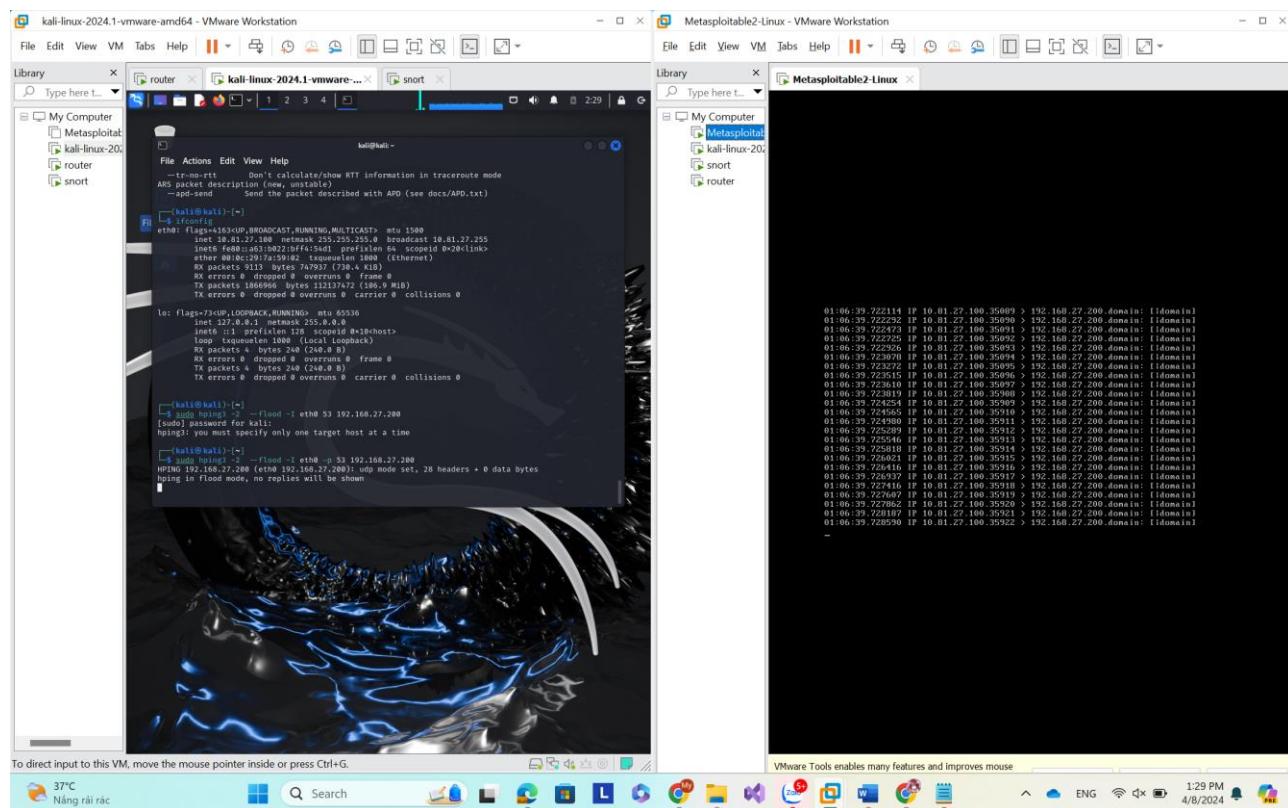
- Snort rules:

drop udp any any -> 192.168.27.200 53 (msg:"over 90 packet per 10 sec for DNS"; threshold: type limit, track by_dst, count 90, seconds 10; sid:1000001; rev:1;)

- Trước khi cài rules:

+ Phía bên attacker thực hiện flood các gói upd dns: sudo hping3 -2 --flood -I eth0 -p 53 192.168.27.200

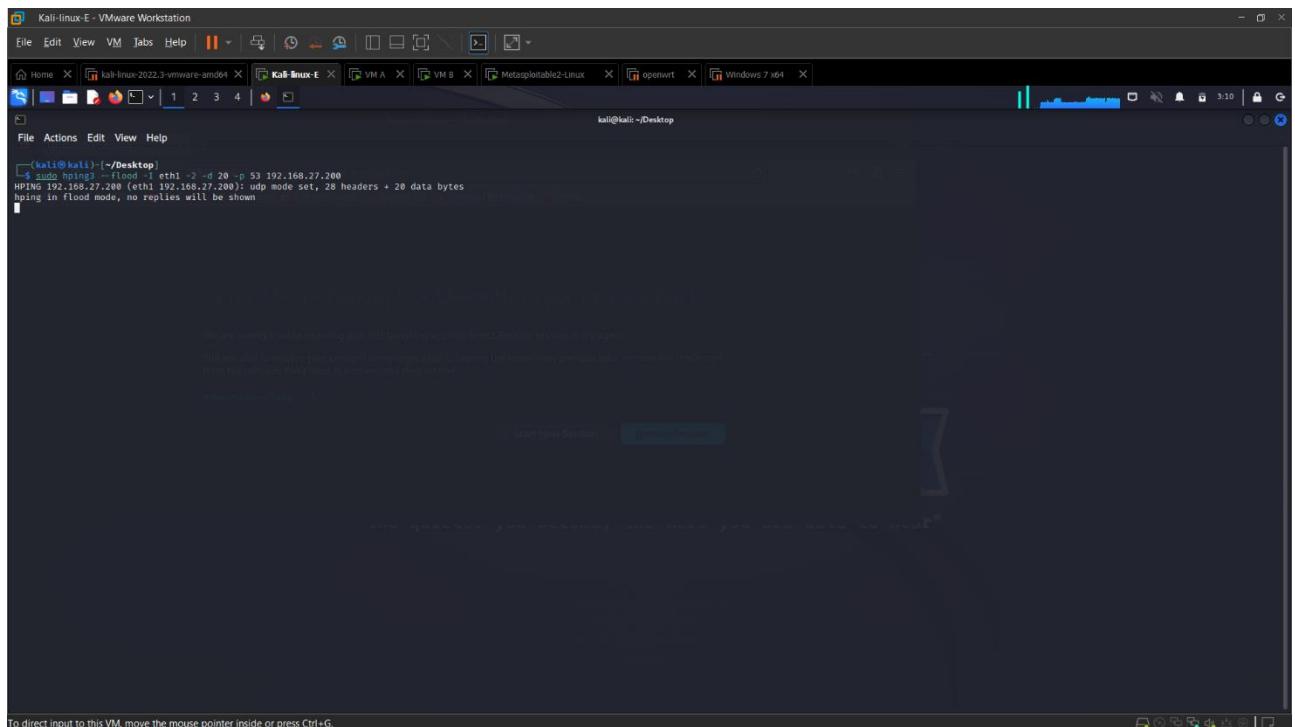
+ Phía bên victim bắt tcpdump, nhận thấy rất nhiều gói tin được truyền đến



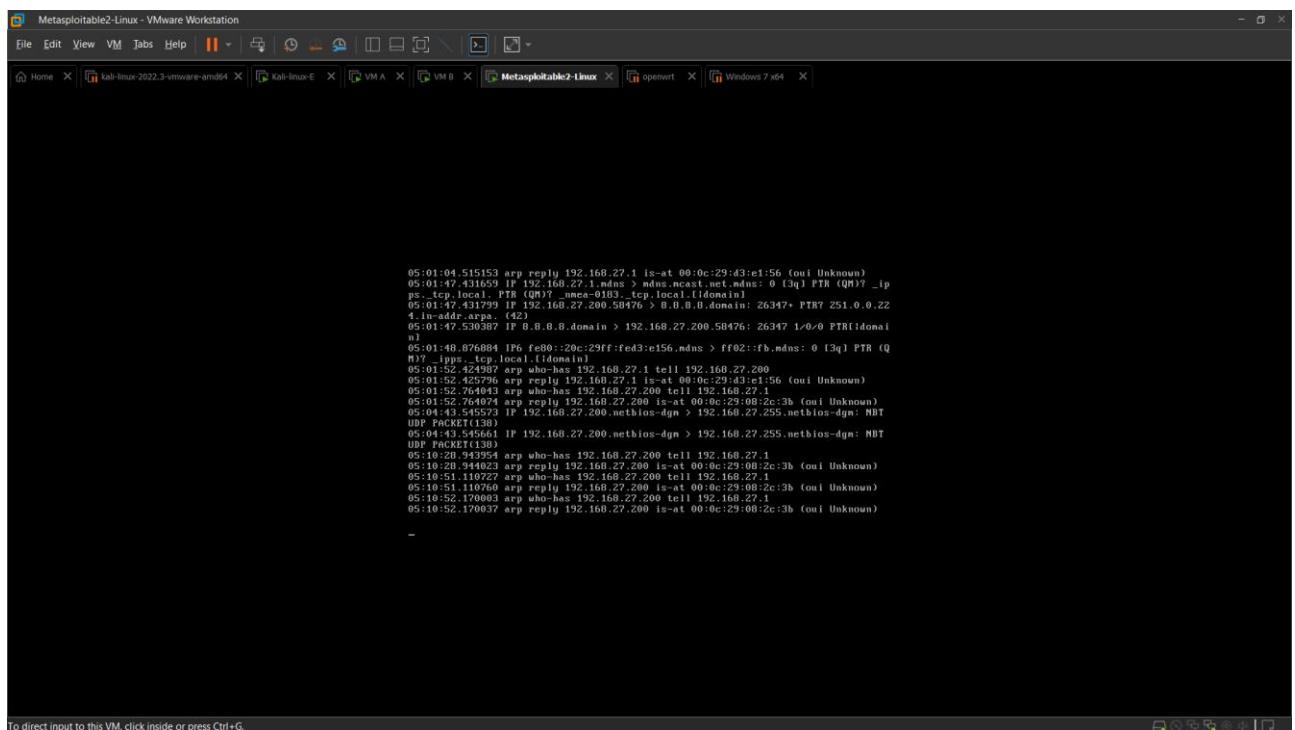
- Sau khi cài rules:

+ Phía bên attacker thực hiện flood các gói upd dns

Lab 03 – Viết rules trên Snort



+ Phía bên victim không hiển thị các gói truy vấn dns liên quan giữa attacker và victim



+ Trong log của snort ghi lại thông tin:

```

VM B - VMware Workstation
File Edit View VM Tabs Help ||| Home kali-linux-2022.3-vmware-amd64 VM A VM B Metasploitable2-Linux openwrt Windows 7 x64
Activities Terminal
root@ubuntu2004: /var/log/snort
root@ubuntu2004:/var/log/snort# tail -n 15 alert
[Priority: 0]
04/08-02:58:51.004894 10.81.27.100:22561 -> 192.168.27.200:53
UDP TTL:63 TOS:0x0 ID:19976 Iplen:20 DgmLen:48
Len: 20
[*] [1:100001:1] over 90 packet per 10 sec for DNS [**]
[Priority: 0]
04/08-02:58:51.004894 10.81.27.100:22561 -> 192.168.27.200:53
UDP TTL:63 TOS:0x0 ID:19976 Iplen:20 DgmLen:48
Len: 20
[*] [1:100001:1] over 90 packet per 10 sec for DNS [**]
[Priority: 0]
04/08-02:58:51.004900 10.81.27.100:22562 -> 192.168.27.200:53
UDP TTL:63 TOS:0x0 ID:34462 Iplen:20 DgmLen:48
Len: 20
root@ubuntu2004:/var/log/snort#

```

To direct input to this VM, click inside or press Ctrl+G.

2. Yêu cầu 1.2: Chỉ cho phép truy cập đến một số dịch vụ: Telnet, FPT, SSH, Web, mail, NetBIOS, SMB, MySQL, postgresql

- Cho phép các máy truy cập đến các port đang mở của máy Victim. Chặn tất cả các port còn lại

- Snort rules:

```

VM B - VMware Workstation
File Edit View VM Tabs Help ||| Home kali-linux-2022.3-vmware-amd64 VM A VM B Metasploitable2-Linux openwrt Windows 7 x64
Activities Terminal
root@ubuntu2004: /var/log/snort
root@ubuntu2004:/var/log/snort# cat /etc/snort/rules/nhom9-snort.rules
drop tcp any --> 192.168.27.200 !SPORT (msg:"TCP Port not allow!!!"; sid: 100001; rev: 1)
drop udp any --> 192.168.27.200 !SPORT (msg:"UDP Port not allow!!!"; sid: 100002; rev: 1)
config daq: afpacket
config daq_mode: inline
include /etc/snort/rules/nhom9-snort.rules
portvar PORT [21,22,28,23,25,80,443,137,138,139,143,445,3306,5432]
root@ubuntu2004:/var/log/snort# 

```

To direct input to this VM, click inside or press Ctrl+G.

- Lab 03 – Viết rules trên Snort

- Trước khi cài rules:

+ Kết quả scan các port và dịch vụ TCP:

+ Bên máy vintim nhận một loạt các gói khi thực hiện quét từ máy attacker:

```
Metasploitable-2-Linux - VMware Workstation
File Edit View VM Tabs Help || □ × [Metasploitable-2-Linux] [spewrt] [Windows 7 x64]

Home X kali-linux-2022.3-vmware-amd64 X Kali-Linux-E X VM A X VM B X Metasploitable-2-Linux X spewrt X Windows 7 x64 X

05:26:16.601182 IP 192.168.27.200.53107 > 10.81.27.100.38532: R 0:0(0) ack 12065
79500 win 0
05:26:16.601423 IP 10.81.27.100.46314 > 192.168.27.200.32217: S 2735723458:273573
458(0) win 64240 <ms 1460.sackOK.timestamp 301170132 0.nop.uscale ?>
05:26:16.601451 IP 192.168.27.200.32217 > 10.81.27.100.46314: R 0:0(0) ack 27357
3459 win 0
05:26:16.601470 IP 10.81.27.100.33916 > 192.168.27.200.19405: S 3032244795:30262
44735(0) win 64240 <ms 1460.sackOK.timestamp 301170132 0.nop.uscale ?>
05:26:16.601779 IP 192.168.27.200.19405 > 10.81.27.100.33916: R 0:0(0) ack 30262
44736 win 0
05:26:16.602105 IP 10.81.27.100.53704 > 192.168.27.200.5941: S 20484595522:204845
8522(0) win 64240 <ms 1460.sackOK.timestamp 301170132 0.nop.uscale ?>
05:26:16.602132 IP 192.168.27.200.5941 > 10.81.27.100.53704: R 0:0(0) ack 204845
0523 win 0
05:26:16.602334 IP 10.81.27.100.55266 > 192.168.27.200.18257: S 3546117953:25461
17900 win 0
05:26:16.602340 IP 192.168.27.200.18257 > 10.81.27.100.55266: R 0:0(0) ack 25461
17964 win 0
05:26:16.602606 IP 10.81.27.100.45426 > 192.168.27.200.31609: S 1105292914:11052
5231(0) win 64240 <ms 1460.sackOK.timestamp 301170133 0.nop.uscale ?>
05:26:16.604070 IP 192.168.27.100.33992 > 192.168.27.200.29010: S 3037330787:30373
3087(0) win 64240 <ms 1460.sackOK.timestamp 301170134 0.nop.uscale ?>
05:26:16.605103 IP 10.81.27.100.41380 > 192.168.27.200.9349: S 3578160626:3578160
26(0) win 64240 <ms 1460.sackOK.timestamp 301170134 0.nop.uscale ?>
```

Lab 03 – Viết rules trên Snort

+ Kết quả scan các port và dịch vụ UDP:

```

kali@kali:~$ sudo nmap -sU -T4 -p 100 192.168.27.200
[sudo] password for kali:
Starting Nmap 7.94SWN ( https://nmap.org ) at 2024-04-08 03:43 EDT
Nmap scan report for 192.168.27.200
Host is up (0.00002s latency).
Not shown: 53 closed TCP ports (port-unreach), 43 open|filtered UDP ports (no-response)
PORT      STATE SERVICE
53/udp    open  domain
111/udp   open  rpcbind
137/udp   open  netbios-ns
2049/udp  open  nfs

Nmap done: 1 IP address (1 host up) scanned in 44.97 seconds

```

- Sau khi cài rules:

+ Kết quả scan các port và dịch vụ TCP: chỉ trả về các port liên quan đến các dịch vụ được phép truy cập, số lượng ít hơn so với trước khi áp dụng rules

```

kali@kali:~$ sudo nmap -sT -T4 -p 100 192.168.27.200
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-08 03:34 EDT
Nmap scan report for 192.168.27.200
Host is up (0.00002s latency).
Not shown: 65534 filtered TCP ports (no-response)
PORT      STATE SERVICE
20/tcp    closed  ftp-data
21/tcp    open   ftplib
22/tcp    open   ssh
23/tcp    open   telnet
25/tcp    open   smtp
80/tcp    open   http
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open   netbios-ssn
143/tcp   closed imap
445/tcp   open   microsoft-ds
3306/tcp  open   mysql
5432/tcp  open   postgresql

Nmap done: 1 IP address (1 host up) scanned in 104.81 seconds

```

+ Trong log của snort ghi lại thông tin:

```

root@ubuntu2004:/var/log/snort
[*][1:100001:1] TCP Port not allow!!! [**]
[Priority: 0]
04/08/03 16:27:00.10:81.27.200:59900 -> 192.168.27.200:59900
TCP|L4|143 TOS:t0x0 ID:3755 Iplen:20 DgmLen:60 DF
*****S* Seq: 0x0355F6E Ack: 0x0 WIn: 0xFAB0 TcpLen: 48
TCP Options (S) => MSS: 1460 SackOK TS: 301780391 0 NOP WS: 7

[*][1:100001:1] TCP Port not allow!!! [**]
[Priority: 0]
04/08/03 16:27:00.10:81.27.200:47868 -> 192.168.27.200:46538
TCP|L4|143 TOS:t0x0 ID:3575 Iplen:20 DgmLen:60 DF
*****S* Seq: 0x048AD48F2 Ack: 0x0 WIn: 0xFAB0 TcpLen: 48
TCP Options (S) => MSS: 1460 SackOK TS: 301780391 0 NOP WS: 7

[*][1:100001:1] TCP Port not allow!!! [**]
[Priority: 0]
04/08/03 16:27:00.10:81.27.200:58298 -> 192.168.27.200:51614
TCP|L4|143 TOS:t0x0 ID:43243 Iplen:20 DgmLen:60 DF
*****S* Seq: 0x03352F00 Ack: 0x0 WIn: 0xFAB0 TcpLen: 48
TCP Options (S) => MSS: 1460 SackOK TS: 301780392 0 NOP WS: 7

root@ubuntu2004:/var/log/snort#

```

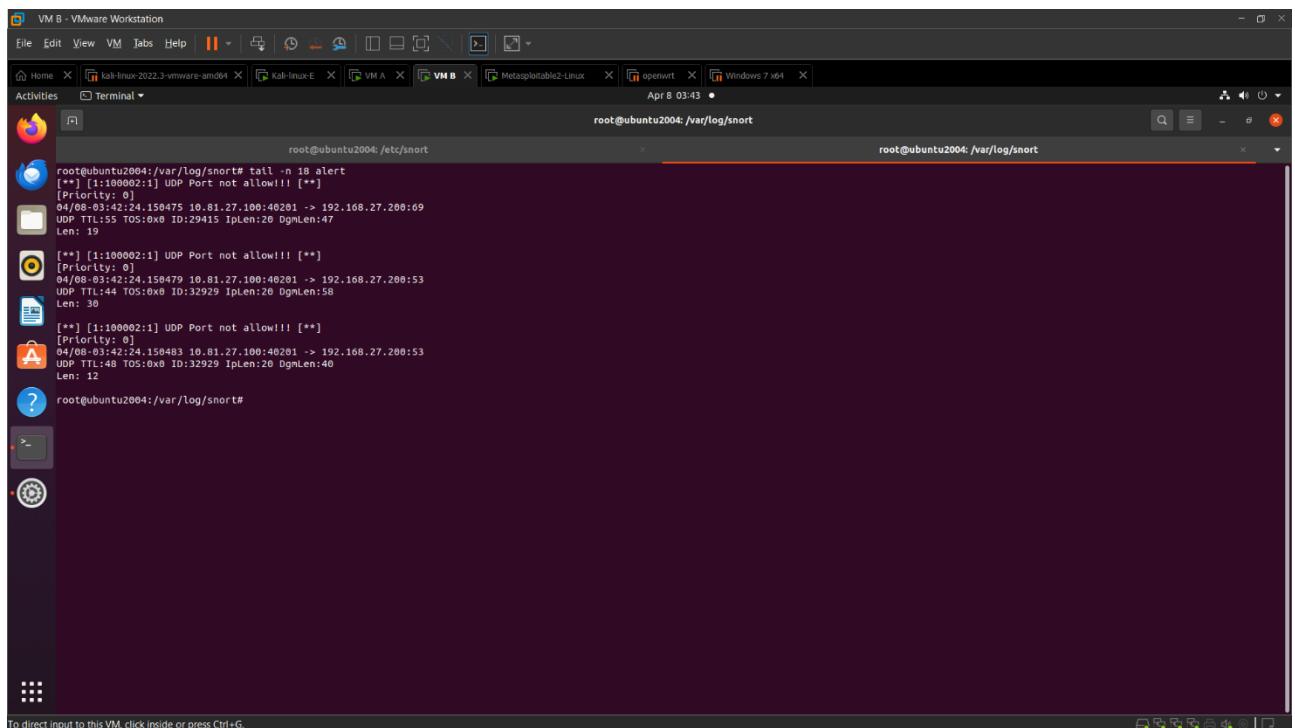
+ Kết quả scan các port và dịch vụ UDP: chỉ trả về các port liên quan đến các dịch vụ được phép truy cập, số lượng ít hơn so với trước khi áp dụng rules:

```

File Actions Edit View Help
-0/-O/-o<file>: Output scan in normal, XML, s|<script Kiddi3,
and Grepable format, respectively, to the given filename.
--append-output: Append to the specified output file
-v: Increase verbosity level (use -vv or more for greater effect)
-d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--script: Run a specific script
--open: Open all ports (or port range) in parallel
--socket-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--append-output: Append to rather than clobber specified output files
--resume: Continue an aborted scan
--interactive: Disable keyboard interactions via keyboard
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
--enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datafile <name>: Specify custom Nmap data file location
--datadir <dir>: Specify custom Nmap data file location
--script <script>: Run a specific script
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -IR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
(kali㉿kali):~/Desktop
$ nmap -PU -oX - 192.168.27.200
Sorry, UDP Ping (-PU) only works if you are root (because we need to read raw responses off the wire)
QUITTING!
(kali㉿kali):~/Desktop
$ nmap -PU -oX - 192.168.27.200
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-08 03:42 EDT
Nmap scan report for 192.168.27.200
Host is up (0.0003s latency).
Not shown: 95 open|filtered udp ports (no-response)
PORT      STATE SERVICE
80/udp    close http
22/udp    close ssh
23/udp    close telnet
139/udp   closed netbios-ssn
445/udp   closed microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 2.29 seconds
(kali㉿kali):~/Desktop
$ 

```

+ Trong log của snort ghi lại thông tin:



```
root@ubuntu2004:/var/log/snort# tail -n 18 alert
[*] [1:100002:1] UDP Port not allow!!! []
[Priority: 0]
04/08/03:42:24.158475 10.81.27.100:40281 -> 192.168.27.200:69
UDP TTL:35 TOS:0x0 ID:29415 IpLen:20 DgmLen:47
Len: 10

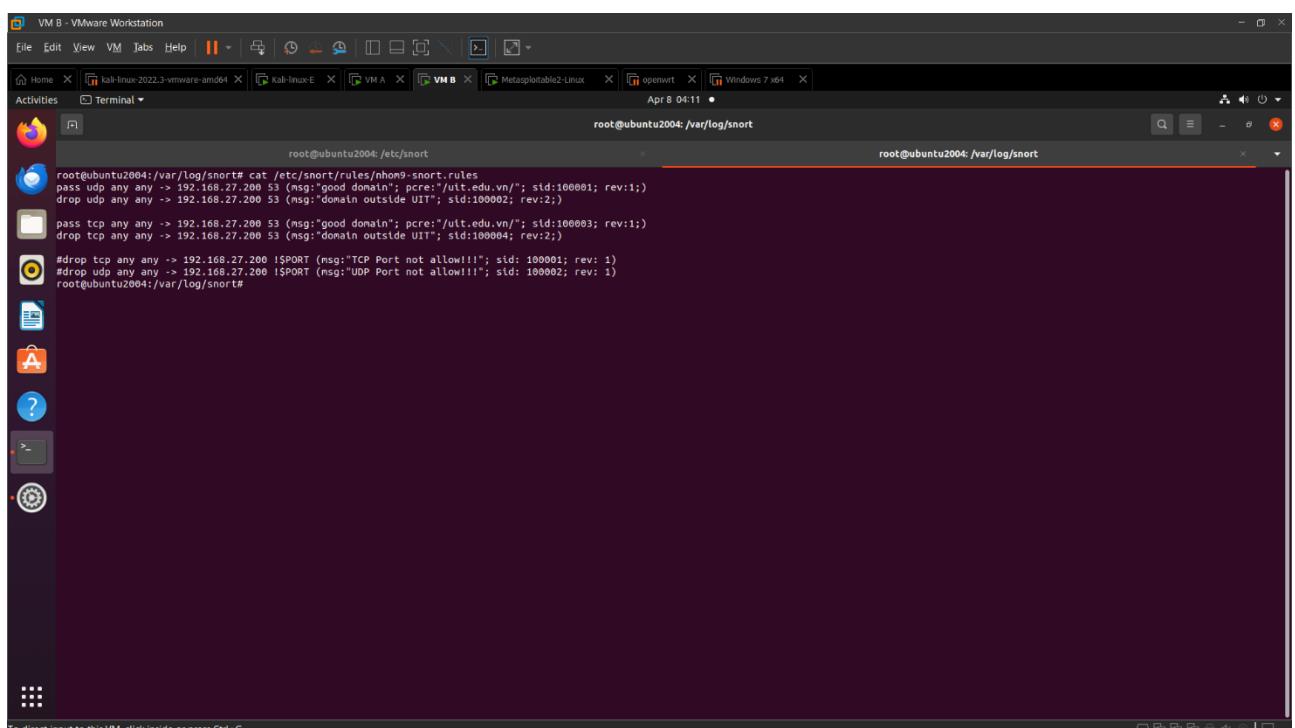
[*] [1:100002:1] UDP Port not allow!!! []
[Priority: 0]
04/08/03:42:24.158479 10.81.27.100:40281 -> 192.168.27.200:53
UDP TTL:44 TOS:0x0 ID:32929 IpLen:20 DgmLen:58
Len: 30

[*] [1:100002:1] UDP Port not allow!!! []
[Priority: 0]
04/08/03:42:24.158483 10.81.27.100:40281 -> 192.168.27.200:53
UDP TTL:48 TOS:0x0 ID:32929 IpLen:20 DgmLen:40
Len: 12

root@ubuntu2004:/var/log/snort#
```

3. Yêu cầu 1.3: Chỉ cho phép truy vấn DNS đến các miền thuộc quản lý của UIT

- Snort rules:



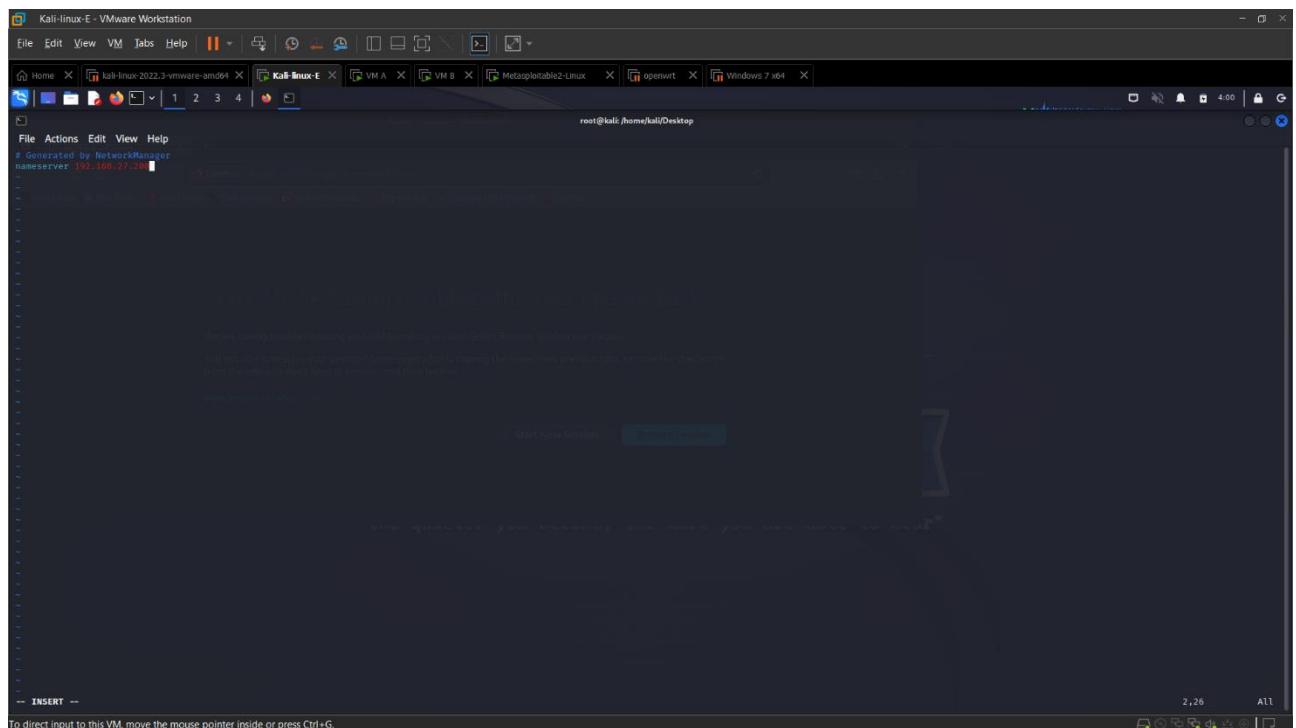
```
root@ubuntu2004:/var/log/snort# cat /etc/snort/rules/nhom9-snort.rules
pass udp any any -> 192.168.27.200 53 (msg:"good domain"; pcre:"uit.edu.vn/"; sid:100001; rev:1;)
drop udp any any -> 192.168.27.200 53 (msg:"domain outside UIT"; sid:100002; rev:2;)

pass tcp any any -> 192.168.27.200 53 (msg:"good domain"; pcre:"uit.edu.vn/"; sid:100003; rev:1;)
drop tcp any any -> 192.168.27.200 53 (msg:"domain outside UIT"; sid:100004; rev:2;)

#drop tcp any any -> 192.168.27.200 !SPORT (msg:"TCP Port not allow!!!"; sid: 100001; rev: 1)
#drop udp any any -> 192.168.27.200 !$PORT (msg:"UDP Port not allow!!!"; sid: 100002; rev: 1)
root@ubuntu2004:/var/log/snort#
```

Lab 03 – Viết rules trên Snort

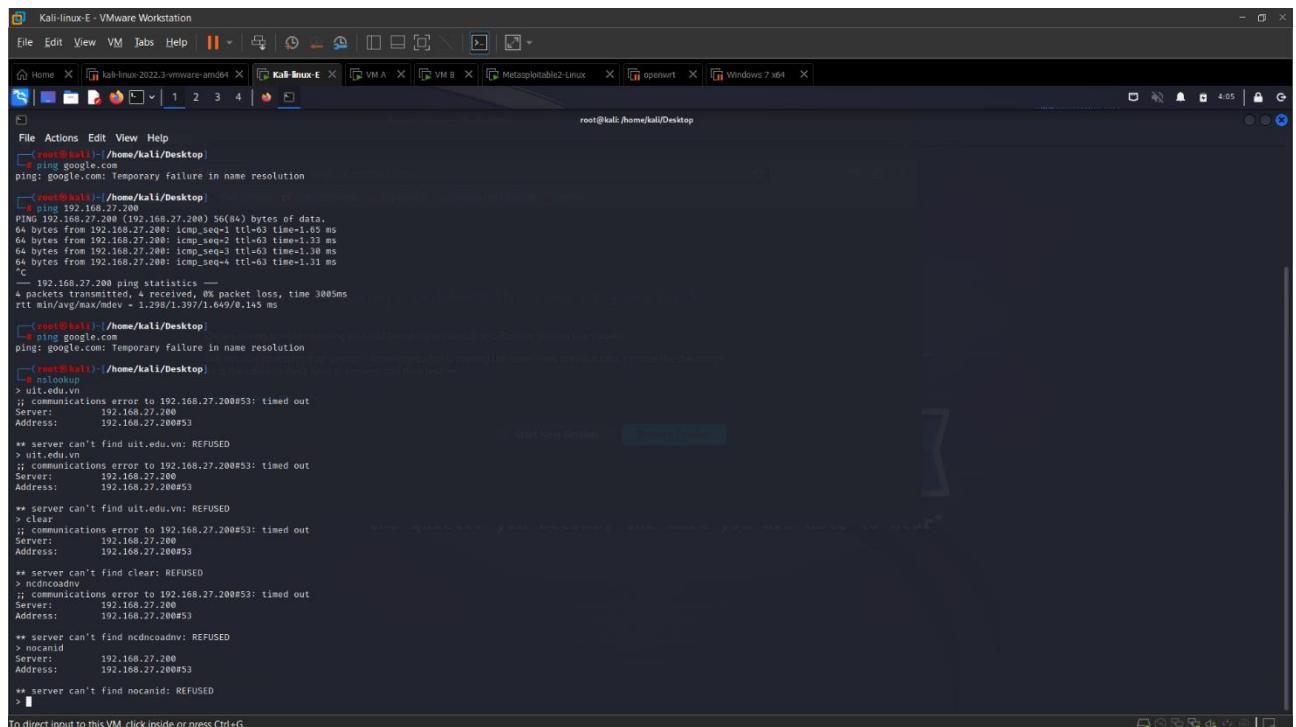
+ Ngoài ra, tiến hành chỉnh lại nameserver:



- Trước khi cài rules: Thực hiện nslookup luôn nhận được kết quả

Server: 192.168.27.200

Address: 192.168.27.200#53



Lab 03 – Viết rules trên Snort

- + Bên máy victim nhận và phản hồi refuse với mọi thực hiện nslookup

```

06:05:52.631945 IP 192.168.27.200.domain > 10.81.27.100.50877: 58749 Refused- 0/
0.0 (23)
06:05:52.632011 IP 192.168.27.200.domain > 10.81.27.100.53635: 58749 Refused- 0/
0.0 (23)
06:05:52.632699 IP 10.81.27.100 > 192.168.27.200: ICMP 10.81.27.100 udp port 50877 unreachable, length 59
06:06:10.378572 IP 10.81.27.100.37367 > 192.168.27.200.domain: 65500+ #? ncndcos domain#<
06:06:10.378725 IP 192.168.27.200.domain > 10.81.27.100.37367: 65500 Refused- 0/
0.0 (28)
06:06:10.378771 IP 10.81.27.100.42386 > 192.168.27.200.domain: 65500+ #? ncndcos domain#<
06:06:10.378847 IP 192.168.27.200.domain > 10.81.27.100.42386: 65500 Refused- 0/
0.0 (28)
06:06:10.379860 IP 10.81.27.100 > 192.168.27.200: ICMP 10.81.27.100 udp port 373 unreachable, length 64
06:06:11.530695 IP 10.81.27.100.34601 > 192.168.27.200.domain: 62204+ #? nocanid (25)
06:06:11.530852 IP 192.168.27.200.domain > 10.81.27.100.34601: 62204 Refused- 0/
0.0 (28)
06:06:15.374986 arp who-has 192.168.27.1 tell 192.168.27.200
06:06:15.375006 arp reply 192.168.27.1 is-at 00:0c:29:43:1e:56 (oui Unknown)
06:06:15.477595 arp who-has 192.168.27.200 tell 192.168.27.1
06:06:15.477629 arp reply 192.168.27.200 is-at 00:0c:29:08:2c:3b (oui Unknown)

```

To direct input to this VM, click inside or press Ctrl+G.

- Sau khi cài rules:

- + Chỉ khi thực hiện nslookup với các miền thuộc uit.edu.vn mới nhận được kết quả:

Server: 192.168.27.200

Address: 192.168.27.200#53

```

root@kali:~#
> nslookup
; communications error to 192.168.27.200#53: timed out
Server:      192.168.27.200
Address:      192.168.27.200#53

** server can't find ncndcoady: REFUSED
> nocamid
Server:      192.168.27.200
Address:      192.168.27.200#53

** server can't find nocamid: REFUSED
> google.com
; communications error to 192.168.27.200#53: timed out
Server:      192.168.27.200
Address:      192.168.27.200#53

** server can't find google.com: REFUSED
> example.com
; communications error to 192.168.27.200#53: timed out
Server:      192.168.27.200
Address:      192.168.27.200#53

; communications error to 192.168.27.200#53: timed out
; communications error to 192.168.27.200#53: timed out
; communications error to 192.168.27.200#53: timed out
; no servers could be reached

> uit.edu.vn
Server:      192.168.27.200
Address:      192.168.27.200#53

** server can't find uit.edu.vn: REFUSED
> das.uit.edu.vn
; communications error to 192.168.27.200#53: timed out
Server:      192.168.27.200
Address:      192.168.27.200#53

** server can't find das.uit.edu.vn: REFUSED
> google.com
; communications error to 192.168.27.200#53: timed out
; communications error to 192.168.27.200#53: timed out
; communications error to 192.168.27.200#53: timed out
; no servers could be reached
> 

```

To direct input to this VM, click inside or press Ctrl+G.

```

06:08:34.056671 arp who-has 192.168.27.1 tell 192.168.27.200
06:08:34.057549 arp reply 192.168.27.1 is-at 00:0c:29:43:c1:56 (oui Unknown)
06:08:34.240223 arp who-has 192.168.27.200 tell 192.168.27.1
06:08:34.240259 arp reply 192.168.27.200 is-at 00:0c:29:00:2c:3b (oui Unknown)
06:09:58.221096 arp who-has 192.168.27.200 tell 192.168.27.1
06:09:58.221096 arp reply 192.168.27.200 is-at 00:0c:29:08:2c:3b (oui Unknown)
06:10:27.745176 10.81.27.100.35693 > 192.168.27.200.domain: 37337+ RTT mit.edu
    .vn. (28)
06:10:32.746190 IP 192.168.27.200.domain > 10.81.27.100.35695: 37337 Refused- 0/
06:10:32.746190 arp who-has 192.168.27.1 tell 192.168.27.200
06:10:32.746783 arp reply 192.168.27.1 is-at 00:0c:29:43:c1:56 (oui Unknown)
06:10:32.746783 IP 10.81.27.100.35413 > 192.168.27.200.domain: 2779+ RTT das.uit.
.edu.vn. (32)
06:10:35.509142 IP 10.81.27.100.56928 > 192.168.27.200.domain: 2779+ RTT das.uit.
.edu.vn. (32)
06:08:04:12:02.738969 IP 192.168.27.200.domain > 10.81.27.100.35413: 2779 Refused- 0/0
    .edu.vn. (32)
06:10:35.511014 IP 192.168.27.200.domain > 10.81.27.100.56928: 2779 Refused- 0/0
    .edu.vn. (32)
06:10:35.512340 IP 10.81.27.100 > 192.168.27.200: ICMP 10.81.27.100 udp port 354
13 unreachable, length 68
06:10:40.723228 arp who-has 192.168.27.200 tell 192.168.27.1
06:10:40.723228 arp reply 192.168.27.200 is-at 00:0c:29:08:2c:3b (oui Unknown)

```

+ Trong log của snort ghi lại thông tin:

```

root@ubuntu2004:/var/log/snort# tail -n 30 alert
[*] [i:1:00002:2] domain outside UIT [*]
[Priority: 0]
04/08-04:12:02.738969 10.81.27.100:55878 -> 192.168.27.200:53
    UDP TTL:63 TOS:0x0 ID:61461 Iplen:26 DgnLen:71 DF
    Len: 43
[*] [i:1:00002:2] domain outside UIT [*]
[Priority: 0]
04/08-04:12:02.744169 10.81.27.100:56772 -> 192.168.27.200:53
    UDP TTL:63 TOS:0x0 ID:14152 Iplen:26 DgnLen:71 DF
    Len: 43
[*] [i:1:00002:2] domain outside UIT [*]
[Priority: 0]
04/08-04:12:02.744185 10.81.27.100:56772 -> 192.168.27.200:53
    UDP TTL:63 TOS:0x0 ID:14153 Iplen:26 DgnLen:71 DF
    Len: 43
[*] [i:1:00002:2] domain outside UIT [*]
[Priority: 0]
04/08-04:12:12.749007 10.81.27.100:56772 -> 192.168.27.200:53
    UDP TTL:63 TOS:0x0 ID:14154 Iplen:26 DgnLen:71 DF
    Len: 43
[*] [i:1:00002:2] domain outside UIT [*]
[Priority: 0]
04/08-04:12:12.749651 10.81.27.100:56772 -> 192.168.27.200:53
    UDP TTL:63 TOS:0x0 ID:14155 Iplen:26 DgnLen:71 DF
    Len: 43
root@ubuntu2004:/var/log/snort#

```

4. Yêu cầu 1.4: Ngăn chặn tấn công Time-based SQL Injection

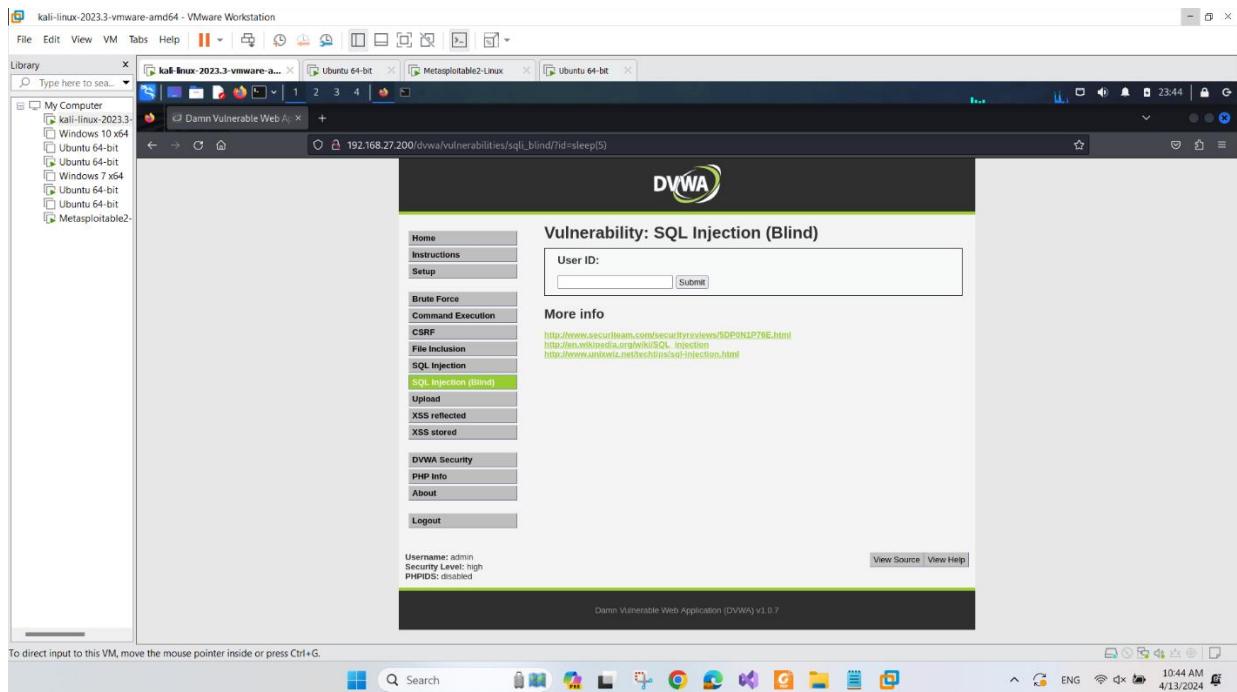
- Snort rules:

`drop tcp any any -> any 80 (msg: "Time-based SQL Injection"; content: "sleep"; nocase; sid:1000005;)`

drop tcp any any -> any 80 (msg: "Time-based SQL Injection"; content: "waitfor delay"; nocase; sid:1000006;)

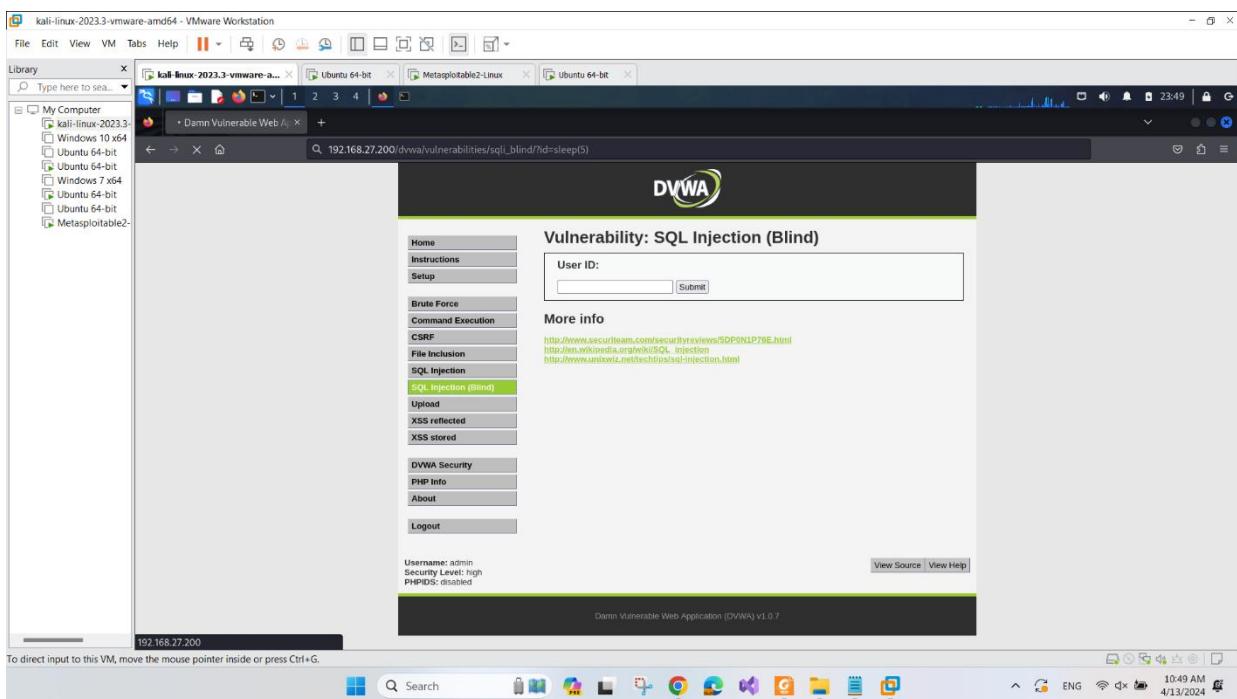
drop tcp any any -> any 80 (msg: "Time-based SQL Injection"; content: "benchmark"; nocase; sid:1000007;)

- Trước khi cài rules: Trang web truy cập bình thường và có thể thực hiện bindshell

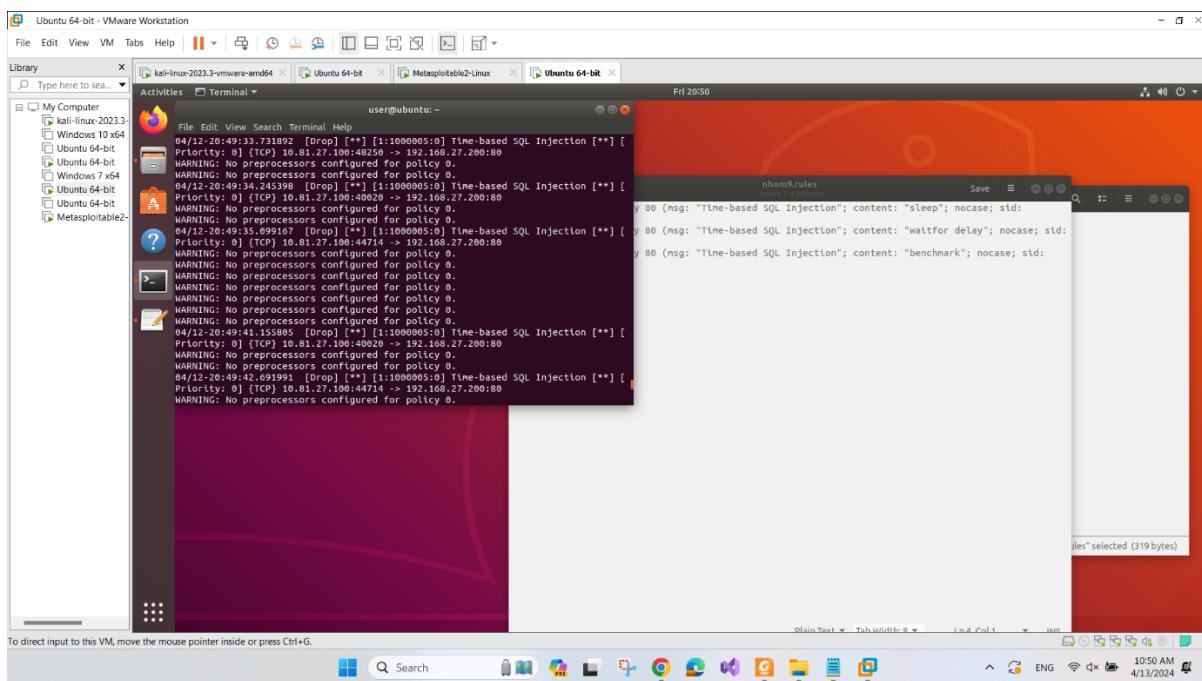


- Sau khi cài rules:

+ Tại trang web, web load trang mãi không vào được:



+ Tại snort, xuất hiện các dòng thông báo:



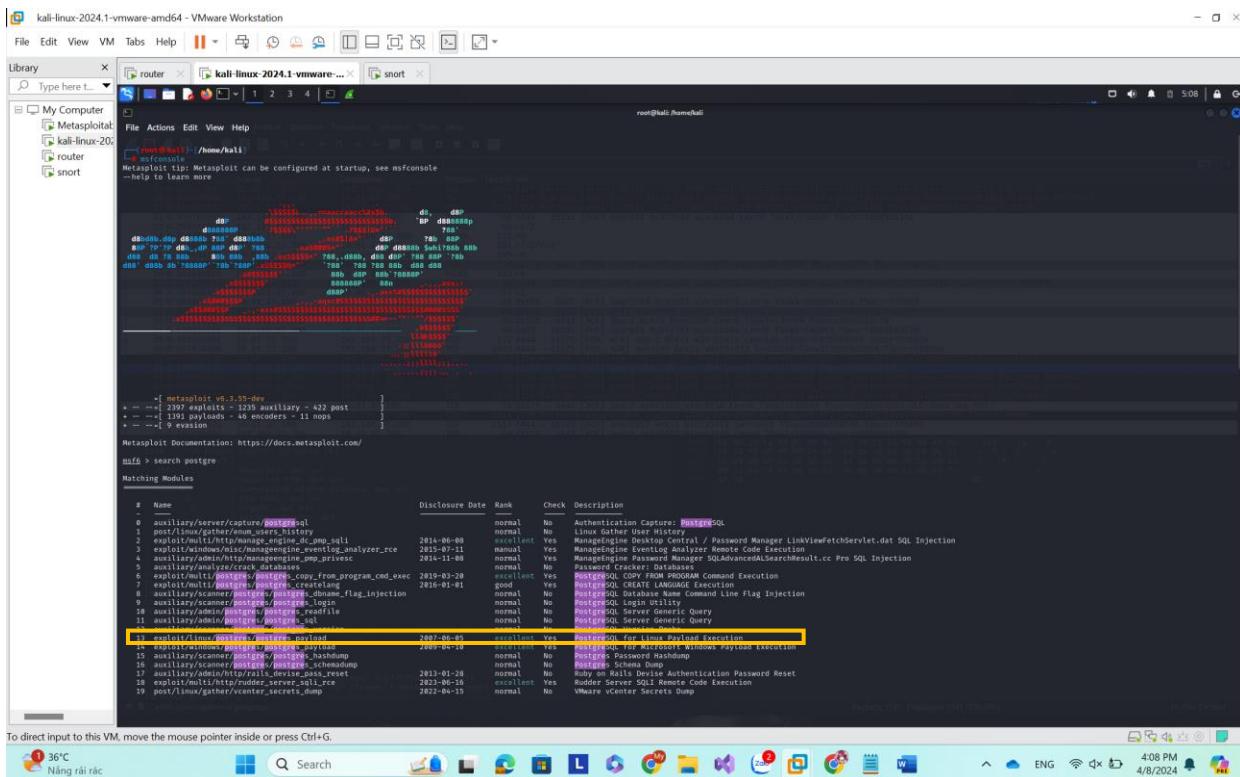
5. Yêu cầu 1.5: Sinh viên tự xây dựng thêm 2 kịch bản tấn công và viết Snort rule để ngăn chặn tấn công

a, Kịch bản 1: PostgreSQL for Linux Payload Execution

Trên một số bản cài đặt PostgreSQL mặc định của Linux, tài khoản dịch vụ postgres có thể ghi vào thư mục /tmp và cũng có thể lấy nguồn Thư viện chia sẻ UDF. Từ đó, cho phép thực thi mã tùy ý. Module này biên dịch một tệp đối tượng dùng chung của Linux, tải nó lên máy chủ đích thông qua phương pháp binary injection UPDATE pg_largeobject và tạo một UDF (user defined function) từ đối tượng dùng chung đó.

- Một số thông tin:

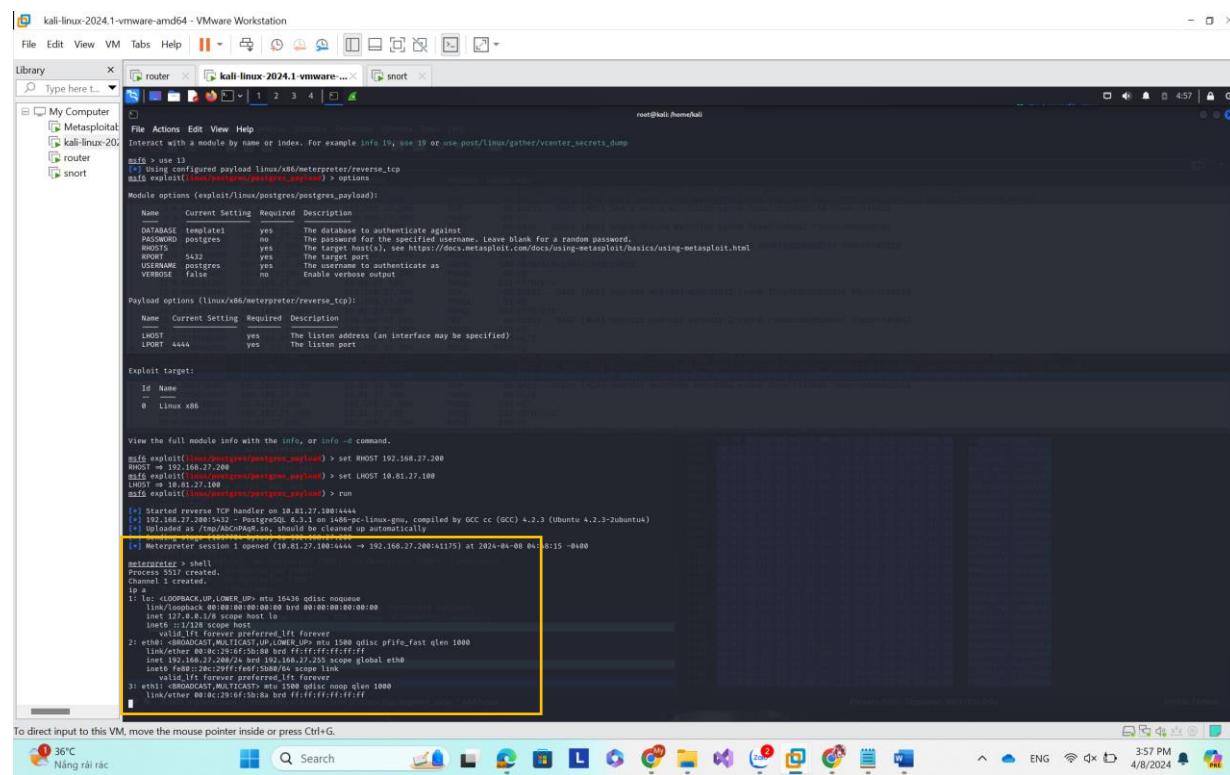
- **Name:** PostgreSQL for Linux Payload Execution
- **Module:** exploit/linux/postgres/postgres_payload
- **Source code:** modules/exploits/linux/postgres/postgres_payload.rb
- **Disclosure date:** 2007-06-05
- **Last modification time:** 2021-08-20 16:06:16 +0000
- **Supported platform(s):** Linux
- **Target service / protocol:** postgres
- **Target network port(s):** 5432
- **List of CVEs:** CVE-2007-3280



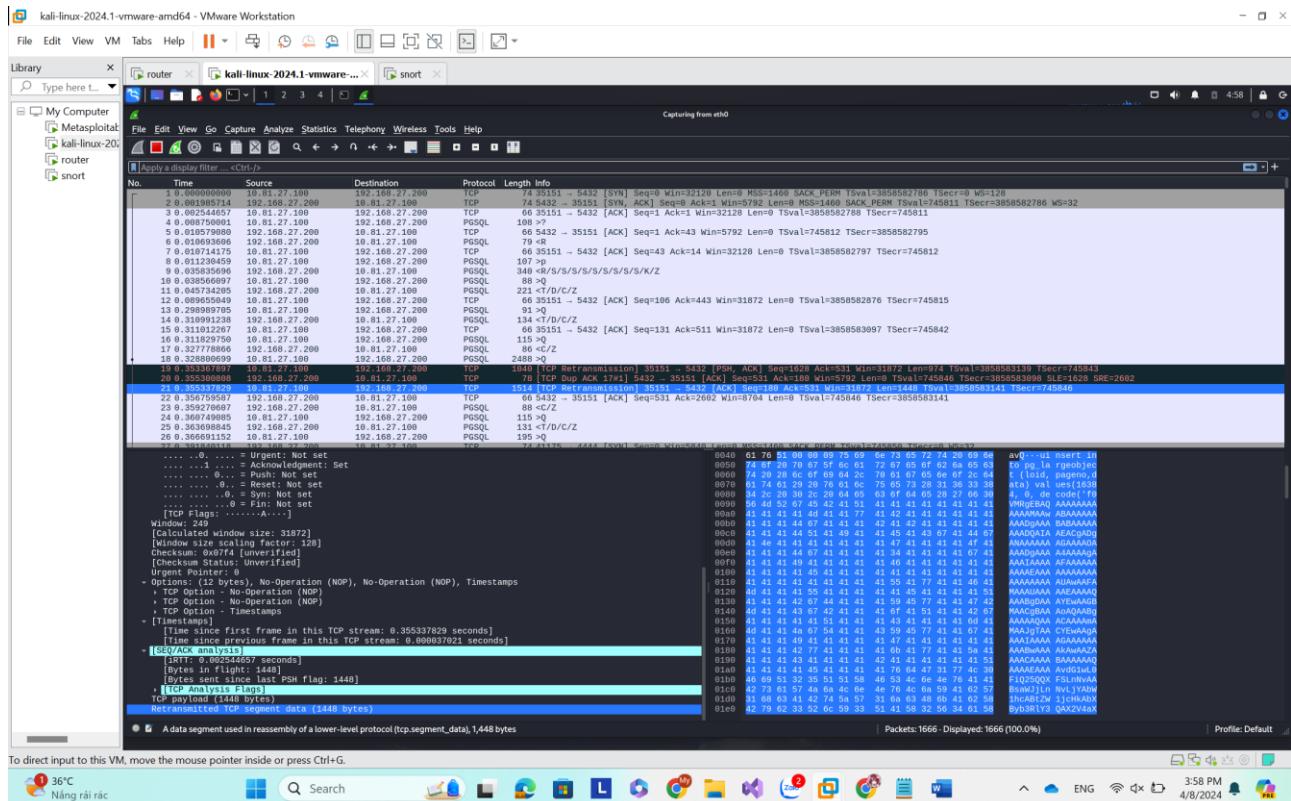
- Snort rules:

```
drop tcp any any -> 192.168.27.200 5432 (msg:"Detected PGSQL!"; content:  
"pg_largeobject"; sid:1000001; rev:1;)
```

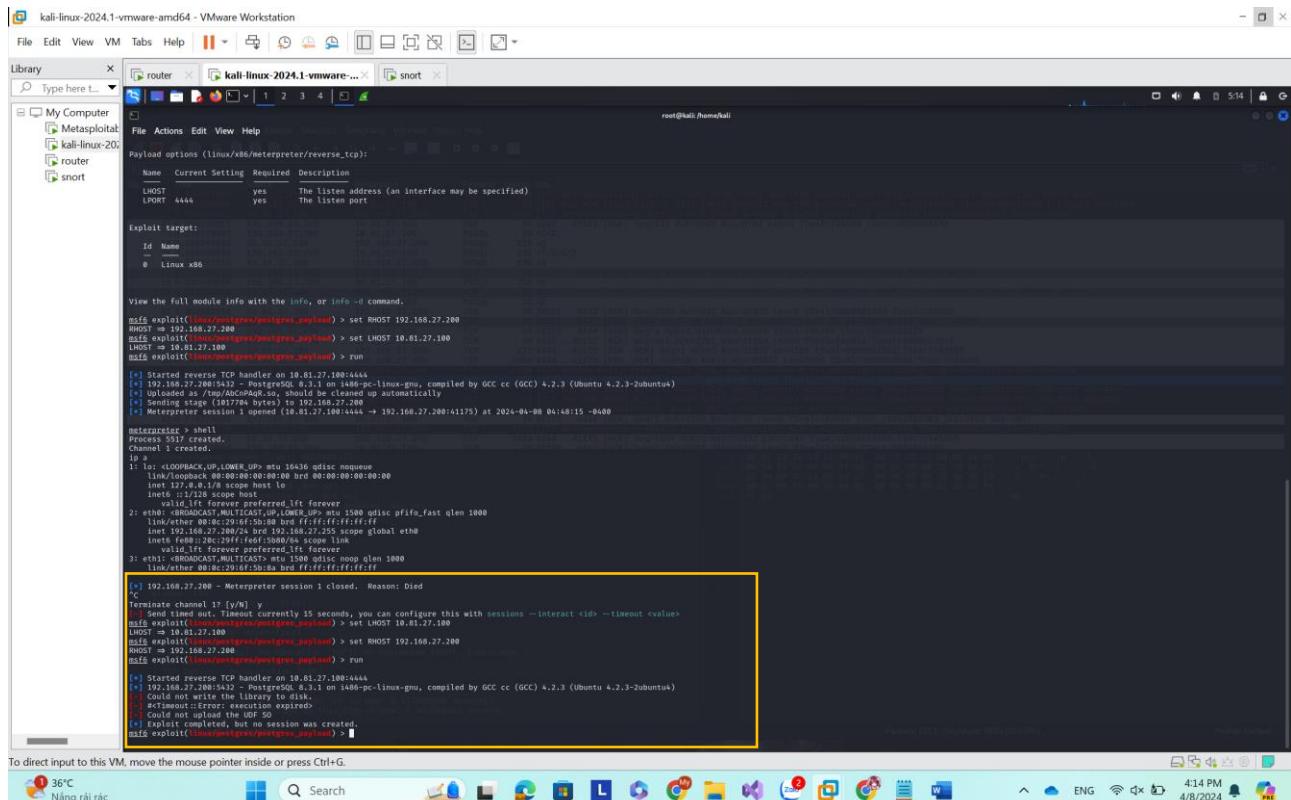
- Trước khi cài rules: Có thể tiến hành khai thác thành công



+ Dùng Wireshark bắt gói, nhận thấy có từ khoá pg_largeobject



- Sau khi cài rules: thất bại khi thực hiện tấn công



+ Tại snort, xuất hiện các dòng thông báo:

```
[**] [!]:1000000111 Detected PGSQL1 [**]
[Priority: 0]
04/12-10:30:02.429335 10.81.27.100:41595 -> 192.168.27.200:5432
TCP TTL:63 TOS:0x0 ID:54821 IpLen:20 DgmLen:101 DF
***>*** Seq: 0x0037F66B Ack: 0xC49AC3BE Win: 0xF9 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3417475716 530576

[**] [!]:1000000111 Detected PGSQL1 [**]
[Priority: 0]
04/12-10:30:02.429335 10.81.27.100:41595 -> 192.168.27.200:5432
TCP TTL:63 TOS:0x0 ID:54821 IpLen:20 DgmLen:101 DF
***>*** Seq: 0x0037F66B Ack: 0xC49AC3BE Win: 0xF9 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3417475716 530576

[**] [!]:1000000111 Detected PGSQL1 [**]
[Priority: 0]
04/12-10:30:12.540823 10.81.27.100:41595 -> 192.168.27.200:5432
TCP TTL:63 TOS:0x0 ID:54827 IpLen:20 DgmLen:101 DF
***>*** Seq: 0x0037F66B Ack: 0xC49AC3BE Win: 0xF9 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3417485828 530576

[**] [!]:1000000111 Detected PGSQL1 [**]
[Priority: 0]
04/12-10:30:12.540823 10.81.27.100:41595 -> 192.168.27.200:5432
TCP TTL:63 TOS:0x0 ID:54827 IpLen:20 DgmLen:101 DF
***>*** Seq: 0x0037F66B Ack: 0xC49AC3BE Win: 0xF9 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3417485828 530576

[**] [!]:1000000111 Detected PGSQL1 [**]
[Priority: 0]
04/12-10:30:53.500442 10.81.27.100:41595 -> 192.168.27.200:5432
TCP TTL:63 TOS:0x0 ID:55429 IpLen:20 DgmLen:101 DF
***>*** Seq: 0x0037F66B Ack: 0xC49AC3BE Win: 0xF9 TcpLen: 32
TCP Options (3) => NOP NOP TS: 3417500708 530576

root@snort:/var/log/snort#
```

b, Kịch bản 2: VNC Authentication Scanner - Exploiting Port 5900 (VNC)

Virtual Network Computing (VNC) chạy trên cổng 5900, dịch vụ này có thể được khai thác bằng cách sử dụng một mô-đun trong Metasploit để tìm thông tin đăng nhập.

- Một số thông tin:

- **Name:** VNC Authentication Scanner
- **Module:** auxiliary/scanner/vnc/vnc_login
- **Source code:** modules/auxiliary/scanner/vnc/vnc_login.rb
- **Disclosure date:** -
- **Last modification time:** 2021-08-31 17:10:07 +0000
- **Supported platform(s):** -
- **Target service / protocol:** -
- **Target network port(s):** 5900, 5901, 5902, 5903, 5904, 5905, 5906, 5907, 5908, 5909, 5910 (theo msfconsole, nó sử dụng port 5900 nên nhóm cũng sẽ trọng tâm ở port 5900).
- **List of CVEs:** CVE-1999-0506

- Snort rules:

```
drop tcp any any -> 192.168.27.200 5900 (msg: "Detected VNC Login!";
sid:1000001; rev:1;)
```

- Trước khi cài rules: nhận được “Login Successful”; đồng thời khi tiến hành mở vncviewer máy victim thành công

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help || File Home snort router kali-linux-2024.1-vmware... Metasploitable2-Linux
File Actions Edit View Help
# Name Disclosure Date Rank Check Description
# aux/scanner/vnc/vnc_login normal No Windows Authentication Scanner
# post/windows/gather/credentials/reconne normal No Windows Gather mRemote Saved Password Extraction

Interact with a module by name or index. For example info 1, use 1 or use post/windows/gather/credentials/reconne

msf6 > use 8
msf6 auxiliary(vnc_login) > options

Module options (auxiliary/scanner/vnc/vnc_login):
Name Current Setting Required Description
ANONYMOUS_LOGIN False yes Attempt to login with a blank username and password
BLANK_PASSWORDS False no Try blank passwords for all users
BROTEXECUTE_SPEED 5 yes Try each user/password couple stored in the list
DB_ALL_CHEATERS false no Add all users in the current database to the list
DB_ALL_USERS false no Add all users in the current database to the list
DB_SKIP_EXISTING none no Skip existing credentials stored in the current database (Accepted: none, usef
PASSWORD /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt no The password to test
PASS_FILE /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt no File containing passwords, one per line
Prives None no A proxy chain of format type:host:port[,type:host:port][...]
PROXY http://127.0.0.1:2087/ yes The proxy to be used for the connection
REPORT 9900 yes Stop guessing when a credential works for a host
STOP_ON_SUCCESS False yes Stop the exploit module execution after a success
THREADS 1 yes Number of threads to use (Accepted: 1-10)
USERNAME <BLANK> no A specific username to authenticate as
USERPASSFILE <BLANK> no File containing users and passwords separated by space, one pair per line
USERFILE <BLANK> no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts

View the full module info with the info, or info -d command.

msf6 auxiliary(vnc_login) > set RHOSTS 192.168.27.200
RHOSTS = 192.168.27.200
msf6 auxiliary(vnc_login) > exploit

[*] 192.168.27.200:5900 - 192.168.27.200:5900 - Starting VNC login sweep
[*] 192.168.27.200:5900 - 192.168.27.200:5900 - No active DB - Credential data will not be saved!
[*] 192.168.27.200:5900 - 192.168.27.200:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] msf6 auxiliary(vnc_login) > quit

[*] msf6 auxiliary(vnc_login) > exit

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

- Sau khi cài rules: nhận được “Login fail”; đồng thời khi tiến hành mở vncviewer máy victim không thành công

```
kali-linux-2024.1-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help || File Home snort router kali-linux-2024.1-vmware... Metasploitable2-Linux
File Actions Edit View Help
# ---[ 9 evasion ]---

Metasploit Documentation: https://docs.metasploit.com/
MSF > search vnc login

Matching Modules

# Name Disclosure Date Rank Check Description
# aux/scanner/vnc/vnc_login normal No Windows Authentication Scanner
# post/windows/gather/credentials/reconne normal No Windows Gather mRemote Saved Password Extraction

Interact with a module by name or index. For example info 1, use 1 or use post/windows/gather/credentials/reconne

msf6 > use 8
msf6 auxiliary(vnc_login) > options

Module options (auxiliary/scanner/vnc/vnc_login):
Name Current Setting Required Description
ANONYMOUS_LOGIN False yes Attempt to login with a blank username and password
BLANK_PASSWORDS False no Try blank passwords for all users
BROTEXECUTE_SPEED 5 yes Try each user/password couple stored in the list
DB_ALL_CHEATERS false no Add all users in the current database to the list
DB_ALL_USERS false no Add all users in the current database to the list
DB_SKIP_EXISTING none no Skip existing credentials stored in the current database (Accepted: none, usef
PASSWORD /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt no The password to test
PASS_FILE /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt no File containing passwords, one per line
Prives None no A proxy chain of format type:host:port[,type:host:port][...]
PROXY http://127.0.0.1:2087/ yes The proxy to be used for the connection
REPORT 9900 yes Stop guessing when a credential works for a host
STOP_ON_SUCCESS False yes Stop the exploit module execution after a success
THREADS 1 yes Number of threads to use (Accepted: 1-10)
USERNAME <BLANK> no A specific username to authenticate as
USERPASSFILE <BLANK> no File containing users and passwords separated by space, one pair per line
USERFILE <BLANK> no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts

View the full module info with the info, or info -d command.

msf6 auxiliary(vnc_login) > set RHOSTS 192.168.27.200
RHOSTS = 192.168.27.200
msf6 auxiliary(vnc_login) > exploit

[*] 192.168.27.200:5900 - 192.168.27.200:5900 - Starting VNC login sweep
[*] 192.168.27.200:5900 - 192.168.27.200:5900 - No active DB - Credential data will not be saved!
[*] 192.168.27.200:5900 - 192.168.27.200:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] msf6 auxiliary(vnc_login) > quit

[*] msf6 auxiliary(vnc_login) > exit

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Lab 03 – Viết rules trên Snort

+ Tại snort, xuất hiện các dòng thông báo:

```

TCP Options (5) => MSS: 1460 SackOK TS: 163918089 0 NOP WS: 7
[*][i:100000011] Detected VNC Login! [*]
[Priority: 0]
04/12-12:18:21.239789 10.81.27.100:37602 -> 192.168.27.200:5900
TOP TTL:63 TOS:0x0 ID:18966 IpLen:20 DgLen:160 IP
*****S* Seq: 0x5A4F6B03 ACK: 0x0 Win: 0x7076 TcpLen: 40
TOP Options (5) => MSS: 1460 SackOK TS: 16392249 0 NOP WS: 7
[*][i:100000011] Detected VNC Login! [*]
[Priority: 0]
04/12-12:18:21.422208 10.81.27.100:37602 -> 192.168.27.200:5900
TOP TTL:63 TOS:0x0 ID:18967 IpLen:20 DgLen:160 IP
*****S* Seq: 0x5A4F6B03 ACK: 0x0 Win: 0x7076 TcpLen: 40
TOP Options (5) => MSS: 1460 SackOK TS: 163930441 0 NOP WS: 7
[*][i:100000011] Detected VNC Login! [*]
[Priority: 0]
04/12-12:18:21.549453 10.81.27.100:37602 -> 192.168.27.200:5900
TOP TTL:63 TOS:0x0 ID:18968 IpLen:20 DgLen:160 IP
*****S* Seq: 0x5A4F6B03 ACK: 0x0 Win: 0x7076 TcpLen: 40
TOP Options (5) => MSS: 1460 SackOK TS: 163946569 0 NOP WS: 7
[*][i:100000011] Detected VNC Login! [*]
[Priority: 0]
04/12-12:18:21.557184 10.81.27.100:37602 -> 192.168.27.200:5900
TOP TTL:63 TOS:0x0 ID:18969 IpLen:20 DgLen:160 IP
*****S* Seq: 0x5A4F6B03 ACK: 0x0 Win: 0x7076 TcpLen: 40
TOP Options (5) => MSS: 1460 SackOK TS: 163960837 0 NOP WS: 7
[*][i:100000011] Detected VNC Login! [*]
[Priority: 0]
04/12-12:19:50.185158 10.81.27.100:52422 -> 192.168.27.200:5900
TOP TTL:63 TOS:0x0 ID:18970 IpLen:20 DgLen:40 IP
*****S* Seq: 0x70890280 ACK: 0x0 Win: 0x0 TcpLen: 20
root@snort:/var/log/snort#_

```

---HẾT---